PURPOSE

To implement procedures that will appropriately guard against the unauthorized modification of Electronic Protected Health Information (ePHI) that is being transmitted over an electronic communications network or via any form of removable media.

DEFINITIONS

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

Encryption means the manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.

PROCEDURE

The possibility of access to ePHI and secure data by individuals who are not the intended recipients of this data will be prevented by encrypting the data, where applicable, by workforce members that are transmitting any ePHI or otherwise secure data.

The encryption method must be Advanced Encryption Standard (AES) compliant, which specifies the federal information processing standards.

REFERENCES

45 CFR 164.308{a)(1)

Advanced Encryption Standard (AES)

Department of Technology, Management and Budget (DTMB) Policy 1315.10 Encryption Standards

DTMB1315.00 Storage of Sensitive Information on Mobile Devices and Portable Media

CONTACT

For more information regarding this procedure, contact the MDHHS Security Officer at MDHHSPrivacySecurity@michigan.gov.